IN THE CLAIMS:

Please rewrite claims 51-54, as follows:

1.-39. (Canceled)

40. (Previously presented) A conditional access method wherein digitized multimedia data are transmitted in a continuous transport stream of successive data packets, comprising the steps of:

- selectively forming an encrypted transport stream from a base transport stream by detecting particular data packets within the base transport stream, removing and then encrypting the particular data packets with an event encryption key having a corresponding event decryption key,

- inserting the encrypted data packets into the remaining base transport stream at insertion positions ahead in time with respect to the original positions of the particular data packets in the base transport system, and

- transmitting the event decryption key to a receiver either with the selectively encrypted data stream or via a mobile telecommunication network prior to broadcasting the multimedia data.

41. (Previously presented) The method of claim 40, further comprising the step of buffering the non encrypted data packets while the particular data packets are encrypted.

42. (Canceled)

43. (Canceled)

44. (Previously presented) The method of claim 40, wherein the event decryption key is transmitted in a Digital Video Broadcast (DVB) environment in specific Entitlement Management Messages (EMMs) protected by a user encryption key, the corresponding user decryption key being provided in the Control Access System (CAS), on a user smart card or on a user Subscriber Identification Module (SIM).

45. (Previously presented) The method of claim 40, wherein said encrypted data packets are inserted at positions which are a predetermined number of data packets ahead of their respective

original positions.

46. (Canceled)

47. (Previously presented) The method of claim 40, wherein the event decryption key is frequently changed.

48. (Previously presented) The method of claim 40, wherein the event decryption key is a fixed key distributed on a pay-per-event basis.

49. (Canceled)

50. (Previously presented) The method of claim 40, further comprising the step of providing the event decryption key which is encrypted using a user encryption key, and providing the corresponding user decryption key to an authorized user.

51. (Currently amended) The method of claim 40, wherein the encrypting step further comprises the step of producing at a head-end encoder the selectively encrypted data stream, wherein the head-end encoder ~~including~~ includes a Common Interface (CI) that in turn has a smart card (SC) interface for a smart card that has encryption circuitry thereon.

52. (Currently amended) The method of claim 40, wherein the encrypting step further comprises the step of producing at a head-end encoder the selectively encrypted data stream, wherein the head-end encoder ~~including~~ includes a Common Interface (CI) for a Personal Computer (PC) card module that has encryption circuitry thereon.

53. (Currently amended) The method of claim 40, wherein the encrypting step further comprises the step of producing at a head-end encoder selectively encrypted data stream, wherein the head-end encoder ~~including~~ includes a PC with an interface for a chip card containing an event encryption key or a user encryption key, the encryption being processed in the PC.

54. (Currently amended) The method of claim 40, wherein the encrypting step further comprises the step of producing at a head-end encoder selectively encrypted data stream, wherein the head-end encoder ~~including~~ includes an encoder module with a Common Interface and Transport Stream (CI&TS) interface to a professional Set-Top-Box (STB).

55. (Previously presented) The method of claim 40, wherein the base data transport stream is a clear data stream.

56. (Previously presented) The method of claim 40, wherein the base transport stream is a DVB-scrambled data stream.

57. (Previously presented) The method of claim 40, wherein all data packets other than the selectively encrypted data packets are Digital Video Broadcast scrambled (DVB-scrambled).

58. (Previously presented) The method of claim 40, wherein every nth data packet of the transport stream is encrypted, n being a fixed number.

59. (Previously presented) The method of claim 40, wherein every nth data packet of the transport stream is encrypted, n being a variable number.

60. (Previously presented) The method of claim 59, wherein the variable number n is randomly variable.

61. (Previously presented) The method of claim 59, wherein the variable number n is variable as a function of data packet contents.

62. (Previously presented) The method of claim 40, further comprising the steps of, at the receiver side :

- receiving the event decryption key by an authorized receiver having a conditional access system,

- receiving selectively the encrypted transport stream by the receiver,

- detecting the encrypted data packets by the conditional access system,

- removing the encrypted data packets from the received transport stream,

- decrypting the encrypted data packets with the event decryption key, and

- inserting the decrypted data packets into the remaining received transport stream at positions corresponding to the respective original positions of the particular data packets within the base transport stream.

63. (Previously presented) The method of claim 62, comprising the step of storing by the conditional access system into a buffer memory, clear data packets while decrypting an encrypted data packet.

64. (Previously presented) The method of claim 62, wherein said conditional access system includes a chip card with decryption circuitry thereon.

65. (Previously presented) The method of claim 64, wherein the chip card is a Subscriber Identification Module (SIM) card.